

## 05/10/26

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-58510

(P2003-58510A)

(43) 公開日 平成15年2月28日 (2003.2.28)

(51) Int.Cl.<sup>7</sup>

識別記号

F I

テ-マ-ト\* (参考)

G 0 6 F 15/00

3 3 0

G 0 6 F 15/00

3 3 0 Z

5 B 0 7 6

1/00

17/60

1 4 2

5 B 0 8 5

17/60

1 4 2

3 0 2 E

5 J 1 0 4

3 0 2

5 1 0

5 1 0

5 1 2

審査請求 未請求 請求項の数10 O L (全 26 頁) 最終頁に続く

(21) 出願番号

特願2001-246398(P2001-246398)

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番  
1号

(72) 発明者 丸山 秀史

神奈川県川崎市中原区上小田中4丁目1番  
1号 富士通株式会社内

(72) 発明者 畠山 卓久

神奈川県川崎市中原区上小田中4丁目1番  
1号 富士通株式会社内

(74) 代理人 100074099

弁理士 大曾 義之 (外1名)

最終頁に続く

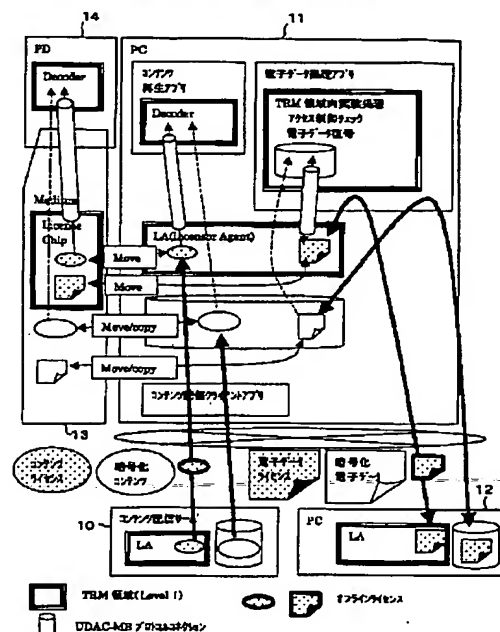
(54) 【発明の名称】 ライセンスのオフライン環境下における送信流通システム及び送信流通方法

(57) 【要約】

【課題】 電子データのライセンスをオフライン化し、ライセンスの安全を守りながら、利用者の利用に便利なライセンスの送信・流通システムを提供する。

【解決手段】 電子データのライセンスを利用するPC 11、12や、コンテンツ配信サーバ10、PD 14にセットされる媒体13は、LA (あるいは、同機能のLicense Chip) を内蔵する。そして、コンテンツや電子データは、ライセンスに基づいて暗号化して、相互にやりとりされるが、ライセンスは、LA間のみで安全な通信方法でやりとりするようにする。これにより、ライセンスの管理を正しく行うと共に、ライセンスの移動を可能にする。

本発明の実施形態の全体構成を示す図



## 【特許請求の範囲】

【請求項 1】暗号化コンテンツのライセンスをユーザ間で流通する際に用いる情報端末であって、暗号化コンテンツのライセンスを格納する第 1 の格納手段と、オフラインライセンスの生成ログを格納する第 2 の格納手段と、暗号化コンテンツのライセンスからオフラインライセンスを生成し、オフラインライセンスから暗号化コンテンツのライセンスを生成して前記第 1 の格納手段に格納し、オフラインライセンス毎に生成ログを作成または更新して前記第 2 の格納手段に格納するライセンスエージェント手段と、を備え、該オフラインライセンスを他の情報端末のライセンスエージェント手段との間でやりとりすることによって、コンテンツのライセンスを送信または受信することを特徴とする情報端末。

【請求項 2】前記ライセンスエージェント手段は TRM 領域内にあることを特徴とする請求項 1 に記載の情報端末。

【請求項 3】前記ライセンスエージェント手段は、ユーザが使用可能なライセンスの複製が生成されずに同一のオフラインライセンスを生成可能であることを特徴とする請求項 1 又は 2 に記載の情報端末。

【請求項 4】前記ライセンスエージェント手段は、オフラインライセンス受信時に、前記生成ログを用いて、移動済みのライセンスが再度格納されることを防止することを特徴とする請求項 1 ～ 3 のいずれか 1 つに記載の情報端末。

【請求項 5】暗号化された放送信号を用いて複数の視聴者に対して同報されるコンテンツのライセンスを受信する際に用いる情報端末であって、コンテンツのライセンスを格納する格納手段と、受信したオフラインライセンスからコンテンツのライセンスを生成し、前記格納手段に格納するライセンスエージェント手段と、を備え、前記放送信号には全視聴契約者のオフラインライセンスが適当な間隔で挿入され、前記情報端末に対応するオフラインライセンスから、暗号化された放送信号を参照可能にするためのライセンスを生成することを特徴とする情報端末。

【請求項 6】情報端末を用いて暗号化コンテンツのライセンスをユーザ間で流通する方法であって、暗号化コンテンツのライセンスを第 1 の格納手段に格納するステップと、前記格納された暗号化コンテンツのライセンスからオフラインライセンスを生成するステップと、前記オフラインライセンスの生成ログを作成または更新して第 2 の格納手段に格納するステップと、

前記オフラインライセンスを他の情報端末に送るステップとを有するライセンスの流通方法。

【請求項 7】情報端末を用いて暗号化コンテンツのライセンスをユーザ間で流通する方法であって、オフラインライセンスを他の情報端末から受け取るステップと、

受け取ったオフラインライセンスから暗号化コンテンツのライセンスを生成するステップと、

前記生成したライセンスを第 1 の格納手段に格納するステップと、

前記オフラインライセンスの生成ログを作成または更新して第 2 の格納手段に格納するステップと、

を有することを特徴とするライセンスの流通方法。

【請求項 8】暗号化された放送信号を用いて複数の視聴契約者に対して同報されるコンテンツのライセンスを流通する方法であって、

放送信号を暗号化するステップと、

全視聴契約者にそれぞれ対応し、前記暗号化された放送信号を参照可能とするためのライセンスを生成するのに

用いるオフラインライセンスを適当な間隔で挿入した前記放送信号を送信するステップと、を有することを特徴とするライセンスの流通方法。

【請求項 9】暗号化コンテンツのライセンスをユーザ間で流通する方法を情報端末に実現させるプログラムであって、

暗号化コンテンツのライセンスを第 1 の格納手段に格納するステップと、

前記格納された暗号化コンテンツのライセンスからオフラインライセンスを生成するステップと、

前記オフラインライセンスの生成ログを作成または更新して第 2 の格納手段に格納するステップと、

前記オフラインライセンスを他の情報端末に送るステップとを有することを特徴とするライセンスの流通方法を情報端末に実現させるプログラム。

【請求項 10】暗号化コンテンツのライセンスをユーザ間で流通する方法を情報端末に実現させるプログラムであって、

オフラインライセンスを他の情報端末から受け取るステップと、

受け取ったオフラインライセンスから暗号化コンテンツのライセンスを生成するステップと、

前記生成したライセンスを第 1 の格納手段に格納するステップと、

前記オフラインライセンスの生成ログを作成または更新して第 2 の格納手段に格納するステップと、

を有することを特徴とするライセンスの流通方法を情報端末に実現させるプログラム。

## 【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、プログラムなどの

使用ライセンスをオフライン環境下において安全に送信流通するシステムに関する。

#### 【0002】

【従来の技術及び発明が解決しようとする課題】今日、インターネットやコンピュータが普及・発達し、プログラムファイル以外にも音楽データファイルなどをネットワークを介して、販売することが行われつつある。しかし、これらのファイルは、電子データであるため、一旦ダウンロードしてしまうと、複製が容易であり、著作権などの諸権利が容易に侵害されてしまうという問題がある。このような問題に対処するために、これら電子ファイルに対するライセンスの配布と管理のためのシステムを確立することが要求されている。

【0003】従来の技術とその問題点を以下に説明する。

【0004】従来の一般利用者間での電子データの保護流通においては、以下に示すように電子データの作成者は、一旦送付してしまった電子データのアクセスを制御することができない。

#### ・NDA文書の企業間での流通

電子文書などをNDA (Non Disclosure Agreement) を結んだ企業のある特定の範囲の人に配布した場合、その範囲外の人にも複写／印刷されて容易に文書がわたってしまう可能性が高い。

#### ・企業内での検討中資料の配布

検討中資料を関連グループにのみ配布した場合でも、結局、複写／印刷されて、それ以外のメンバーにも広がってしまい、社外にその情報が流出してしまう可能性が高くなる。

【0005】従って、電子データ送付後も作成者の意思がアクセス制御に反映されるための機能が必要である。

【0006】従来技術では、上記問題に対する対処として図17のような専用のデータ転送システムを使用している。

【0007】図17は、従来のライセンスを管理するための専用データ転送システムを示す図である。

【0008】同図において、PC（ユーザ端末）の内、コンテンツの送信元では、データ転送専用クライアント装置を使用して、転送すべきコンテンツに転送処理して、専用サーバに専用の機密保護転送方式によって転送する。当該コンテンツを受信する他のユーザのPC（利用者1）では、やはり専用のクライアント装置を有しており、専用サーバから専用の機密保護転送方式によって当該コンテンツを受信する。そして、転送処理することによって、ローカルなハードディスクなどに当該コンテンツを格納すると共に、後に参照などが可能となるようにする。

【0009】このコンテンツを利用者1が、当該コンテンツを利用者2に転送しようとする場合には、やはり、専用クライアント装置の転送処理機能によって当該コン

テンツを専用サーバに専用の機密保護転送方式を用いて転送し、利用者2は、専用サーバから専用の機密保護転送方式を用いて、当該コンテンツを専用のクライアント装置にダウンロードするという形態をとっている。

【0010】図17のシステムの問題点を以下に示す。

1) 電子データ転送には必ず専用のクライアントを使用しなくてはならず、従って、そのクライアントの仕様に縛られた形でしか送信できない（例えば、利用者間のアプリで送受信する、といったことはできない）。

10 【0011】また、電子データの送信は必ず専用サーバを介さなくてはならない。従って、例えば、既存の e-mail の送信可能範囲と同じ範囲の利用者と送受信可能とするためには、理論的には、上記専用サーバがメールサーバと同じだけ普及する必要があるが、そのようなことは現実的ではない。

2) アクセス制御の対象はPCであり、従って、受信した電子データを可搬記録媒体で持ち回り、別のPCで参照する、ということができない。

20 3) 電子データの参照機能自体はなんら保護されていない。従って、メモリの内容やSWAP域の内容から生の電子データを比較的容易に取り出せてしまい、重要な機密データの送信に適しているとはいえない。

【0012】また、一般利用者間での有料コンテンツのライセンス移動としては、以下の点が指摘される。

【0013】インターネット、携帯電話網（PHS網を含む）を介して有料コンテンツを配信するサービスが徐々に開始されているが、これら現状のサービスでは、利用者は、有料コンテンツのライセンスを上記サービスを介して購入するしかなく、一旦購入したライセンスを

30 （コンテンツ並びにライセンスの不正な複写をされることなく）他の利用者に譲渡する、といったことができない。この結果、ネットワーク上でのライセンスの販売経路が非常に限定されたものになり、有料コンテンツの販売元の立場からすると以下に代表される機会損失がされなかった。－利用者が他の利用者に自分のライセンスを譲渡することができない。

【0014】一人の利用者がとりあえずライセンスを購入し、知り合いの中でまわして利用するような場合（各利用者はコンテンツを利用してみて買いたければ買う）。

【0015】上記の問題点についての解決策は現時点では何も考えられていない。すなわち、従来は不正にコンテンツが複写されてしまうようなサービスしかなかった。従って、有料コンテンツがネットワーク上で配信されにくい状況となっていた。

#### 【0016】・有料コンテンツのマルチキャスト

有料コンテンツのマルチキャストの従来の方式では、コンテンツ受信側固有の秘密鍵をコンテンツ送信側とコンテンツ受信側との間で持ち合い、コンテンツ送信側はライセンスをその秘密鍵で暗号化したものとライセンスで

暗号化されたコンテンツを送信している。コンテンツ受信側固有の秘密鍵は IC カードなどの TRM 領域に格納して送信側から利用者に渡される。従って、利用者は、この秘密鍵を取り出すことはできない。

【0017】コンテンツ送信側は、暗号化したコンテンツに全ての受信先用の暗号化ライセンスをつけて送信する。

【0018】図 18 は、従来の有料コンテンツのマルチキャストの仕組みを示す図である。

【0019】送信側では、コンテンツをスクランブル鍵でスクランブルし、これを暗号化コンテンツとしていた。また、スクランブル鍵は、ライセンスによって暗号化される。ライセンスは、秘密鍵 1、・・・n でそれぞれ暗号化され、暗号化ライセンス 1～n とされていた。そして、送信側から受信機に送信する送信データとしては、暗号化コンテンツ、暗号化スクランブル鍵、暗号化ライセンス 1～n である。これをインターネットや、BS/CS などの衛星放送などでマルチキャストする。

【0020】受信機では、IC カードが組み込まれており、受信した暗号化ライセンス i を秘密鍵 i で復号し、ライセンスを取り出す。そして、受信した暗号化スクランブル鍵を取り出されたライセンスで復号化して、スクランブル鍵を得る。これらを IC カード内で行う。そして、受信した暗号化コンテンツを復号化したスクランブル鍵でデスクランブルし、コンテンツを取り出している。

【0021】しかし、上記 IC カードを使ったシステムにおいても以下のような問題点がある。

1) 利用者にとって IC カードの所持は不便

利用者は IC カードの発行を受け、それを保持していないと放送を受信できない。しかも、契約している配信業者（放送局など）の数だけ IC カードを保持していなくてはならない（IC カードに送信側と共用している秘密鍵が入っているため）。利用者にとってはこれは不便である。

2) 相互運用性の問題（IC カードを利用しないケース）

上記のように IC カードに秘密鍵を閉じこめている場合は、配信業者の IC カードの仕様が統一されていれば、1つの受信機で複数の配信業者の送信データを受信することができる（上記のように配信業者の数だけ IC カードが必要になるが）。

【0022】IC カードを利用しないケースでは、受信機と送信側との間で秘密鍵を共用することになり、1つの受信機で複数の配信業者からのコンテンツを受信可能とするのは現実的でなくなる。

【0023】本発明の課題は、電子データのライセンスをオフライン化し、ライセンスの安全を守りながら、利用者の利用に便利なライセンスの送信・流通システムを提供することである。

【0024】

【課題を解決するための手段】本発明のシステムは、電子文書などのコンテンツのライセンスをユーザ間で送信流通するシステムであって、該ライセンスを格納する情報端末は、TRM 領域内にあり、オフラインライセンスを生成・保持し、暗号化コンテンツを第 1 の格納手段に格納し、オフラインライセンス毎に生成ログを保持・更新するライセンスエージェント手段と、暗号化コンテンツを格納する第 1 の格納手段と、生成ログを格納する第 2 の格納手段とを備え、該オフラインライセンスを複数の情報端末の該ライセンスエージェント手段間でのみ、やりとりすることによって、コンテンツのライセンスを送信流通することを特徴とする。

【0025】本発明の方法は、電子文書などのコンテンツのライセンスをユーザ間で送信流通する方法であって、該ライセンスを格納する情報端末における処理は、TRM 領域内にあり、オフラインライセンスを生成・保持し、暗号化コンテンツを第 1 の格納ステップで格納し、オフラインライセンス毎に生成ログを保持・更新するライセンスエージェントを用いてオフラインライセンスを管理するステップと、暗号化コンテンツを格納する第 1 の格納ステップと、生成ログを格納する第 2 の格納ステップとを備え、該オフラインライセンスを複数の情報端末の該ライセンスエージェント間でのみ、やりとりすることによって、コンテンツのライセンスを送信流通することを特徴とする。

【0026】本発明によれば、ライセンスエージェントにおいて、オフラインで流通するライセンスを管理し、ライセンスエージェント間においてのみライセンスを移動可能とすることにより、流通性があり、しかも安全な、オフラインでのライセンスの流通送信を可能とすることができる。

【0027】

【発明の実施の形態】以下において、TRM 領域内にあるライセンスを送付先の公開鍵とセッション鍵を使って第三者がライセンスを取り出せないように暗号化して一般電子ファイルの形で取り出す機能を暗号化ファイルのオフラインライセンスという。

【0028】なお、TRM 領域とは、Tamper Resistant Module 領域のことを言い、領域内のデータを外部から取り出しにくくした領域を言う。詳しくは後述する。

【0029】以下において、ライセンス毎に全てのオフラインライセンス生成ログを生成し、オフラインライセンス格納時にそれを使って既に移動済みのライセンスが再度格納されることを防ぐために使用されるオフラインライセンス生成ログを LRL (License Revocation List) と呼ぶ。

【0030】以下、本発明の実施形態について説明する。

50 【0031】・オフラインライセンスの導入

ライセンスのやりとりを行うための公知の技術としてUDAC-MBがある。

【0032】UDAC-MBでは、ライセンスはTRM領域の中で保持し、TRM間でのライセンスの転送はUDAC-MBプロトコルで規定しているセキュアなコネクション上で行う、というのが基本である。

【0033】そこで規定しているライセンスの転送プロトコルは転送元と転送先との間で複数回のメッセージの送受信を必要としており、オンラインでのリアルタイム双方向通信環境でしか実現できない。従って、以下のケースには不向きであった。

—個人間での一般電子データ（ワード文書など）の送付  
—個人間での有料コンテンツのライセンスの譲渡  
個人間でのデータのやりとりはオフラインが基本であり、オンラインでのリアルタイム通信を強要するのは非現実的（利用者にとって不便であり、かつ広まりにくい）である。

—有料コンテンツとライセンスをセットで媒体（CDなど）に格納して販売

オンラインライセンスを販売する場合は、UDAC-MB準拠の配信システム、あるいはUDAC-MB準拠の可搬記録媒体が不可欠であった。

—コンテンツのマルチキャスト（放送など）

送信側は一方的にコンテンツを送信し、受信側は一方的に受信するケース。

【0034】ライセンスをTRM間でオフラインでやりとり可能とすれば、オフライン環境で電子データや有料コンテンツにそのライセンスを同梱して送ることが可能となり、また、放送などの1方向通信で通信データ内にライセンスを同梱して送ることが可能となる。以降、このライセンスを”オフラインライセンス”と呼ぶ。（それに対して、UDAC-MBで規定しているライセンスを”オンラインライセンス”と呼ぶ。）

オンライン：1つの通信コネクション（socketなど）の中でライセンスの移動、配信を完了させる方式。

【0035】オフライン：送信側と受信側とがコネクションを持たない状態でライセンスの移動、配信を行う方式。つまり、ライセンスを一般電子データの形でネットワーク上であるいは一般可搬記録媒体で流通可能とする方式。

【0036】ここで、オンラインライセンスはUDAC-MB準拠の可搬記録媒体により移動可能であるが、一般電子データの形では扱えない。

【0037】図1は、本発明の実施形態の全体構成を示す図である。

【0038】同図においては、オフラインライセンスの生成後のライセンスとコンテンツの流通の形態を示している。

【0039】各PCやコンテンツ配信サーバ、PD（Private DeviceあるいはPortable Device）にセットさ

れる媒体には、LA（Licensor Agentあるいは、LAをチップ化したLicense Chip）が組み込まれているものとする。LAについては、後述する。

【0040】コンテンツ配信サーバ10のLA内を用いて、コンテンツのライセンスが送信される。また、コンテンツ配信サーバ10のハードディスクなどの媒体には暗号化コンテンツが格納される。コンテンツ配信サーバ10は、PC11に対し、コンテンツライセンスを、そのLAに対して送信し、暗号化コンテンツをその媒体に送信する。PC11のコンテンツ再生アプリでは、LAに受信されたコンテンツライセンスを用いて、媒体に格納された暗号化コンテンツをTRM領域内に有るデコーダによってデコードし再生する。また、PC12から電子データをPC11が電子文書などの電子データを受け取る場合には、PC12のLAから送信された電子データライセンスをPC11のLAにおいて受け取り、暗号化電子データを媒体に受け取る。そして、PC11では、電子データ処理アプリのTRM領域内実装処理を用いて、電子データライセンスを処理し、これを用いて電子データの復号を行う。電子データライセンスの処理とは、アクセス制御チェックなどである。なお、PC11内のLAとコンテンツ再生アプリのデコーダあるいは電子データ処理アプリのTRM領域内実装処理との通信はUDAC-MBプロトコルを用いる。UDAC-MBプロトコルは公知であるので、ここでは特に説明しないが、実施形態の説明の最後に列挙されている各特許出願を参照されたい。

【0041】PC11から、暗号化コンテンツや暗号化電子データを媒体13に移動し、この媒体をPD14に設定することによって、PD14でコンテンツや電子データを使用することも可能である。この場合、媒体13には、License Chipが搭載され、暗号化コンテンツ、暗号化電子データは、通常通り移動あるいはコピーされるが、コンテンツライセンス、電子データライセンスは、UDAC-MBプロトコルをつかってTRM領域内にあるLicense Chipに格納される。媒体13がセットされたPD14では、暗号化コンテンツや暗号化電子データを、UDAC-MBプロトコルでLicense Chipから取得したコンテンツライセンスや電子データライセンスでデコードし使用する。PD14のデコーダもTRM領域に含まれている。このように、媒体13に格納可能とすることによって、ライセンスに守られたコンテンツをオフラインで配布することが可能となる。

【0042】なお、ここで、同図では、音楽データなどのコンテンツと電子文書などの電子データとを別個に記載したが、実質的には双方とも電子ファイルであることには変わりなく、以下では、特に区別することなく電子データとコンテンツをほぼ同義で使用する。

【0043】図2及び図3は、LAの機能を説明する図である。

【0044】LAのライセンス・暗号化データ生成機能部では、電子データ（コンテンツ）、コンテンツID、アクセス条件を入力とし、電子データ暗号化処理部に電子データの暗号化処理を、ライセンス生成処理部にライセンスの生成処理を依頼する。ライセンス生成処理部では、トランID制御部（トランザクションID制御部）のトランID採番処理部（トランザクションID採番処理部）に依頼して、ライセンスに一意の番号であるトランIDを取得するように依頼する。このようにして処理された結果、暗号化データがライセンス・暗号化データ生成機能部から出力される。

【0045】オフラインライセンス生成機能部では、送信先LA、個別公開鍵証明書、コンテンツID、トランザクションIDを入力として、ライセンス制御部、LRL制御部にライセンスの確認検索を依頼する。そして、オフラインライセンスを付与することが認められると、オフライントランID制御部のオフライントランID採番処理においてオフラインライセンスに一意のトランザクションIDが取得され、ライセンス制御部のレコードを削除し、LRL制御部のレコードを追加することによって、オフラインライセンスが登録され、暗号化処理を受けた後、オフラインライセンスが発行される。

【0046】オフラインライセンス格納機能部では、オフラインライセンスを入力として、これを復号処理し、ライセンス制御部とLRL制御部に対し、レコードの検索を依頼する。レコード検索の結果、ライセンスが承認されると、LRL制御部において、レコード削除を行い、ライセンス制御部において、レコード追加を行う。このとき、ライセンス制御部及びLRL制御部において、ライセンス管理用データベースやLRL制御用データベースにアクセスする場合には、DBMS (Database Management system) を介して、暗号化してデータの授受を行う。

【0047】また、図3に示される、ライセンス検索機能部においては、コンテンツIDを入力として、ライセンス制御部にレコード検索を依頼する。同時に、LRL制御部にもレコード検索を依頼する。そして、検索の結果として、トランザクションIDとアクセス条件が得られる。

【0048】図4は、オフラインライセンスの構成の概要を示す図である。

【0049】同図において、各Partは、以下のよう

に定義される。

【0050】Part 1: セッション鍵を送信先LAの個別公開鍵で暗号化したもの

Part 2: 以下のデータをセッション鍵で暗号化したもの

—オフラインライセンス生成元（送信元）LAの個別公開鍵証明書サブジェクト名

—オフライントランザクションID

オフラインライセンス生成元（送信元）LAで採番したもの—ライセンス（オンラインライセンス）

—配信先TRM内アクセス条件

オフラインライセンスによる移動可能回数/期間

その他

—コンテンツ再生・電子データ処理システムのTRM内アクセス条件

Part 3: オフラインライセンス生成元（送信元）

LAのクラス秘密鍵による電子署名

Part 4: オフラインライセンス生成元（送信元）

LAの個別公開鍵証明書

Part 5: オフラインライセンス生成元（送信元）

LAのクラス公開鍵証明書

ここで、以下に、UDAC-MB/LBを変更して本実施形態のオフラインライセンスを取り扱うため使用するUDAC-PI (Protocol Independent) の説明を行う。

前提

a) ライセンス配信側は個別公開鍵KPrと秘密鍵Krのペアを持つ。

b) またクラス秘密鍵Kcrで署名されたKPrの証明書C(Kcr, KPr || Ir)を持つ。

c) またルート秘密鍵Karで署名されたKPrの証明書C(Kar, KPr || Iar)を持つ。

d) ライセンス配信先はメディア、ライセンスチップまたはLA内のTRMとする。

e) TRMは個別公開鍵KPtと秘密鍵Ktのペアを持つ。

f) 個別公開鍵KPtはクラス秘密鍵Kctで署名された証明書の形で公開されている。

g) クラス公開鍵KPtはルート秘密鍵Katで署名された証明書の形で公開されている。

h) リスク上問題がなければ、KarとKatの認証局は同じでも良く、KarとKatも同じでも良い。

【0051】全証明書をLDAP (Lightweight Directory Access Protocol) で検索可能であれば、なおいっそう利用者が扱いやすい。

・基本手順

(1) 配信側はLDAPなどの手段を用いて配信先TRMのKPtの証明書を取得する。

(2) KPtの証明書をKPtで、また、その証明書をKPtでチェックする。

(3) 配信側は次の形式のオフラインライセンスを生成する。

$$E(KPt, Ks) || E(Ks, SNr || TransactionID || Kc || ACt || ACp || Is) || E(Kcr, H(all\ plain\ text) || C(Kcr, KPr || Ir) || C(Kar, KPr || Iar))$$

ここで、

K s : セッション鍵  
 S N r : 配信側個別公開鍵 K P r の証明書のサブジェク  
 ト名 (subject name)  
 Transaction I D : ライセンスシリアル番号。配信側が  
 ライセンス毎にユニークな番号を生成  
 K c : コンテンツ鍵  
 A C t : 配信先 T R M 内アクセス条件。A C m と同形  
 式、または、その拡張  
 A C p : 再生システム T R M 内アクセス条件  
 I s : その他の情報  
 H ( x ) : x のハッシュ値  
 C ( K x , K P y ) : 公開鍵 K P y を秘密鍵 K x で署名  
 した証明書  
 | | は、これの前後を単純につなぎ合わせることを示  
 す。  
 (4) 配信側は配信先 T R M にライセンスと暗号化コン  
 テンツを送信する。  
 (5) 配信先 T R M 内でライセンスを復号し、ハッシュ  
 と証明書により内容の正当性をチェックする。  
 (6) 配信先 T R M 内で S N r と Transaction I D がラ  
 イセンス失効リスト (L R L : License Revocation L  
 ist) にないかを確認する。あれば、処理を終了する。  
 (7) 配信先 T R M 内でライセンスの内容をライセンス  
 エントリに格納する。  
 (8) 以降の移動、再生のプロトコル及び手順は U D A  
 C - M B / L B (実施形態の説明の最後の特許出願を参  
 照) と同じ。  
 【0052】オンラインライセンスからのオフラインラ  
 イセンスの生成 (オフライン化)、オフラインライセン  
 スの格納 (オンライン化) は、L A (Licensor Agen  
 t) の機能で実現する。つまり、オフラインライセンス  
 は L A 間でやりとりする。  
 【0053】L A のオフラインライセンス関連機能を以  
 下に示す。  
 - ライセンス情報 (コンテンツ I D、トランザクション  
 I D、アクセス条件、...) 取得機能  
 全ライセンス情報取得  
 該当コンテンツ I D の全ライセンス情報取得  
 - オフラインライセンス生成  
 送信先 L A の個別公開鍵証明書とオンラインライセンス  
 (コンテンツ I D、トランザクション I D) を指定して  
 オフラインライセンスを生成。  
 - オフラインライセンス格納  
 指定されたオフラインライセンスを L A 内のライセンス  
 管理用データベースに格納してオンライン化する。  
 ・コンテンツ再生アプリ、電子データ処理アプリでの T  
 R M 領域内実装処理  
 コンテンツ再生アプリ、電子データ処理アプリでは、以  
 下の一連の処理 (U D A C - M B プロトコル実装処理  
 部) を T R M 領域内で実装する。

- L A (あるいは License Chip) からのオンラインラ  
 イセンスの取得 (U D A C - M B プロトコル)  
 - 暗号化コンテンツ・データをオンラインライセンスを  
 使って復号化  
 - コンテンツの再生、データの処理  
 ・各種公開鍵証明書  
 L A の個別公開鍵証明書と対応する秘密鍵、クラス公開  
 鍵証明書、認証局のルート of 公開鍵証明書は、製造元が  
 個々の L A 毎に製品 (パッケージ) に組み込み、T R M  
 領域内で展開されるようにする。また、L A は自身の個  
 別公開鍵証明書を出力する機能を有する。  
 【0054】利用者は、オフラインライセンスの送信元  
 に自分の L A の個別公開鍵証明書を渡すときは、本機能  
 により取得すればよい。  
 【0055】以下は、本発明の実施形態で使用する既存  
 技術の説明である。  
 【0056】T R M (Tamper Resistant Module)  
 処理内容並びに処理の中で扱っているデータの内容が外  
 から取り出したり推測できないようにする仕組み、並び  
 にその仕組み取り入れた半導体チップやプログラムのこ  
 と。  
 【0057】半導体チップの T R M 化したものをハード  
 ウェア T R M、プログラムを T R M 化したものをソフト  
 ウェア T R M と呼ぶ。本実施形態ではどちらを使用して  
 も良い。  
 1) ハードウェア T R M の方式  
 以下の技術により T R M を実現している。  
 - 外部端子から秘密情報の読み出し・書き換えができな  
 い。制御ファーム、ログ情報、アクセス制御情報などの  
 書き換えができない構造を持たせる。  
 - メタル層、特殊コーティング、メッシュセンサによる  
 シールド。  
 - 極微細化。  
 2) ソフトウェア T R M の方式  
 以下の技術により T R M を実現している。  
 - プログラムの処理とそこで扱うデータの領域を分割  
 し、メモリの中の解析しにくい形で散らばらせる。  
 - ロードモジュールを暗号化しておく。実行の瞬間のみ  
 復号。  
 - 実行のたびにメモリ空間への展開構造が異なるように  
 する。  
 【0058】以下、本実施形態の説明に戻る。  
 【0059】図 5 は、新規ライセンス、暗号化データ生  
 成を説明する図である。  
 【0060】送信元 P C あるいは配信サーバにおいて  
 は、コンテンツ I D とアクセス条件その他を L A のライ  
 センス制御部で受け取ると、トラン ID 制御部におい  
 て、トランザクション I D が与えられ、ライセンス管理  
 用データベースにライセンスが格納される。このライセ  
 ンスは、電子データ暗号/復号機能部において、電子デ

13

ータを暗号化するのに使用される。

ーライセンス管理用データベース

ライセンスを格納するデータベース。実装上はDBMS (Database Management system) を使ってもファイルを使っても良い。

【0061】図6は、ライセンス管理用データベースのレコード構成を示す図である。

各フィールドの説明

・タイムスタンプ1、タイムスタンプ2

レコード作成時のタイムスタンプ。LAは、タイムスタンプ1とタイムスタンプ2とが一致しているか否かによってレコードのファイルへの格納が完了したか否かを判断する。実装において、ライセンス管理用データベースをDBMSを使って実現する場合は、データベースのアトミシディをDBMSが保証するため、このタイムスタンプは無くてもよい。

・コンテンツID

ライセンスに対応するコンテンツのコンテンツID。

・トランザクションID

ライセンスの中に含まれているトランザクションIDとコンテンツIDとでライセンスを一意に識別可能となる。

・暗号化ライセンス

ライセンスを暗号化したもの。LAの秘密鍵で暗号化する。(例えばTDESを使う。) LAの秘密鍵はTRM化された領域内に保持し、他者が参照できないようにする。

・送信元公開鍵証明書サブジェクト名

オフラインライセンスの送付元LAの公開鍵証明書のサブジェクト名。UDAC-MBプロトコル(オンライン)で送られてきた場合は、このフィールドはゼロクリアする。

・オフライントランザクションID1

ライセンスがオフラインライセンスの形で当該LAに送付された場合、オフラインライセンス生成元のLAで採番されたオフライントランザクションIDをここに格納する。オフライントランザクションIDは、オフラインライセンス生成元のLAで一意的な番号を割り振る。送信元公開鍵証明書サブジェクト名とオフライントランザクションIDとでオフラインライセンスが一意に識別可能となる。UDAC-MBプロトコル(オンライン)で送られてきた場合は、このフィールドはゼロクリアする。

【0062】図7は、オフラインライセンスの生成(オフライン化)手順を示す図である。

【0063】送信元PC/配信サーバにおいては、LAのLRL制御部とライセンス制御部にコンテンツIDとトランザクションIDが入力されると、LRL制御部は、LRL制御用データベースを参照し、ライセンス制御部は、ライセンス管理用データベースのライセンスを参照する。LRL制御部は、ライセンス制御部と連絡を

14

取りながら処理を進める。ライセンス制御部の処理結果は、LRL制御部に伝えられると共に、オフライントランザクションID制御部からトランザクションIDがLRL制御部に通知される。そして、LRL制御部からオフラインライセンス暗号/復号制御部にライセンスの暗号化依頼が通知され、暗号化されたオフラインライセンスが出力される。

ーオフライントランザクションID制御部

あるPCのLA(以降、LA1とする)でライセンスの移動を目的としてオフラインライセンスを生成し、そのオフラインライセンスが廻り廻って再びLA1に移動されるケースを想定する。LA1から移動されたライセンスと同じものが間違えて(あるいは不正行為により)再びLA1に格納されようとした場合は、それを防ぐ必要がある。しかしながら、そのライセンスは上記の廻り廻って来たものかもしれず、無条件にはじくことはできない。

【0064】それらのライセンスを識別可能とするために、オフラインライセンス生成時は、オフライントランザクションID制御部においてLA内で一意なIDを新しく割り振る。

ーLRL (License Revocation List) 制御部

オフラインライセンスを生成した場合、その後、LA内のライセンスを回収(削除)する。その場合、再び当該LAに同一のライセンスが格納されるのを防ぐために、オフラインライセンス生成済みのライセンスの情報(送信元個別公開鍵証明書のサブジェクト名、オフラインライセンスIDなど)を保持・管理する。

【0065】なお、ライセンスを配信する配信サーバにおいては、ライセンスの配信を目的としてオフラインライセンスを生成し、ライセンスの移動は行わない。従って、一般に配信サーバではLRL制御部は必要ない。

【0066】図8は、LRL (License Revocation List) 制御用データベースのレコード内容を示す図である。

【0067】以下のフィールド以外はライセンス管理用データベースと全く同じ。

【0068】送信先公開鍵証明書サブジェクト名：当該LAでオフラインライセンスを生成したときの送付先LAの公開鍵証明書のサブジェクト名

オフライントランザクションID2：当該LAでオフラインライセンスを生成したときに採番したオフライントランザクションID。

【0069】最新フラグ：各ライセンス(オンラインライセンス)毎の最新の生成済みオフラインライセンスであることを示すフラグ。

【0070】オン：最新 オフ：最新でない。

【0071】オフラインライセンスを再生成する場合は、このフィールドの値がオンであるレコードの情報を使用する。

ー入力パラメータ

- ・送信先LA個別公開鍵証明書
- ・コンテンツID
- ・トランザクションID

利用者は、予めライセンス表示機能部により、オフラインライセンスを生成するライセンスのコンテンツIDとトランザクションIDを取得しておく。

【0072】ただし、ライセンスに対応する商品の情報は、専用ツールで管理しても良いし、利用者が自分で管理しても良い。図9、及び図10は、LAの動作を説明するフローチャートである。

【0073】まず、ステップS1において、コマンド制御部が、オフラインライセンスの生成機能を起動する。ステップS2において、LA機能のシリアルライズ処理（ロードモジュールの二重起動抑止、セマフォなど）を行う。ステップS3において、送信先LAの個別公開鍵証明書の正当性をチェックする。

【0074】次に、ステップS4において、LRL制御部において、LRL制御用データベースを以下のキーで検索する。

- ーコンテンツID＝入力パラメータ
- ートランザクションID＝入力パラメータ
- ー最新フラグ＝オン

ここで、最新フラグがオンになっている当該ライセンスが存在しない場合には、ライセンス制御部において（ステップS5）、ライセンス管理用データベースを以下のキーで検索する。

- ーコンテンツID
- ートランザクションID

そして、この検索で対応するライセンスがないと判断された場合には、該当ライセンス無しとしてエラー処理をして、ステップS21に進む。対応するライセンスが存在する場合には、オフライントランID制御部において、オフライントランザクションIDの採番が行われる（ステップS6）。そして、ステップS7において、LRL制御部は、ステップS5で検索したレコードの値と入力パラメータの値、並びにオフライントランザクションIDからLRL制御用データベースのレコードを作成して、最新フラグをオンとして格納する。ステップS8では、ライセンス制御部が、ステップS5で検索したライセンス管理用データベースのレコードを削除する。そして、ステップS9において、オフラインライセンス暗号／復号制御部は、ステップS7で作成したレコードの値と入力パラメータからオフラインライセンスを作成し、元へ返して、ステップS21に進む。

【0075】ステップS4において、対応するライセンスがあると判断された場合には、ステップS10において、ライセンス制御部は、ステップS4の検索で利用したコンテンツID、トランザクションIDを使ってライセンス管理用データベースを検索する。対応するライセ

ンスが無い場合には、ステップS11において、ステップS4で検索したレコードの送信先LA個別公開鍵証明書サブジェクト名と入力パラメータの送信先個別公開鍵証明書のサブジェクト名とが等しいか否かを判断する。判断の結果、異なる場合には、該当ライセンスがないというエラーとなり、ステップS21に進む。ステップS11の判断が、等しいとなると、ステップS12において、オフラインライセンス暗号／復号制御部は、ステップS4で検索したレコードの値と入力パラメータからオフラインライセンスを作成し、呼び出しもとへ返して、ステップS21に進む。

【0076】ステップS10において、対応するライセンスが存在すると判断された場合には、図10のステップS13において、ステップS10で検索したレコードの送信元個別公開鍵証明書サブジェクト名、オフライントランザクションID1がステップS4で検索したレコードのそれぞれのフィールドの値と等しいか否かを判断する。等しい場合には、ステップS14において、ステップS4で検索したレコードの送信先LA個別公開鍵証明書サブジェクト名と入力パラメータの送信先個別公開鍵証明書のサブジェクト名とが等しいか否かを判断する。ステップS14の判断で、異なると判断された場合には、該当ライセンス無しというエラーとなり、ステップS21に進む。ステップS14で等しいとなると、ステップS15において、ライセンス制御部が、ステップS10で検索したライセンス管理用データベースのレコードの送信元個別公開鍵証明書サブジェクト名が全てゼロでなければ、そのレコードを削除し、オフラインライセンス暗号／復号制御部が、その後、ステップS4で検索したレコードの値と入力パラメータからオフラインライセンスを作成し、呼び出しもとへ返し、ステップS21に進む。

【0077】ステップS13の判断において、異なると判断された場合には、ステップS16において、LRL制御部が、ステップS4で検索したLRL制御用データベースのレコードの最新フラグの値をオフにし、ステップS17において、オフライントランザクションID採番をオフライントランID制御部が行う。そして、ステップS18において、LRL制御部は、ステップS10で検索したレコードの値と入力パラメータの値、並びにオフライントランザクションIDの値からLRL制御用データベースのレコードを作成する。そして、作成したレコードをLRL制御用データベースに格納（最新フラグをオン）する。ステップS19では、ステップS10で検索したライセンス管理用データベースのレコードを、ライセンス制御部が削除し、ステップS20において、オフラインライセンス暗号／復号制御部は、ステップS18で作成したレコードの値と入力パラメータからオフラインライセンスを作成し、呼び出しもとへ返し、ステップS21に進む。

17

【0078】ステップS21においては、LA機能のシリアルライズ解除を行い、処理を終了する。

【0079】ステップS5、S10のライセンス管理用データベースの検索処理部で該当レコードが存在する場合は、レコード内の暗号化ライセンスを復号し、コンテンツIDとトランザクションIDの値がレコード検索のキーで指定したそれぞれの値と等しくなければ、ライセンス管理用データベースが改竄されたとみなし、エラーで終了する。

【0080】ステップS4のLRL制御部用データベースの検索処理部で該当レコードが存在する場合は、レコード内の暗号化ライセンスを復号し、コンテンツIDとトランザクションIDの値がレコード検索のキーで指定したそれぞれの値と等しくなければ、LRL制御部用データベースが改竄されたとみなし、エラーで終了する。

【0081】ステップS9のオフラインライセンス生成処理部では、ステップS5で検索したレコードの中の暗号化ライセンスを当該LAの内部にある秘密鍵で復号し、その復号した結果を使ってオフラインライセンスを生成する。

【0082】ステップS12、S15のオフラインライセンス生成処理部では、ステップS4で検索したレコードの中の暗号化ライセンスを当該LAの内部にある秘密鍵で復号し、その復号した結果を使ってオフラインライセンスを生成する。

【0083】ステップS20のオフラインライセンス生成処理部では、ステップS10で検索したレコードの中の暗号化ライセンスを当該LAの内部にある秘密鍵で復号し、その復号した結果を使ってオフラインライセンスを生成する。

【0084】図11は、オフラインライセンスの格納（オンライン化）処理を説明する図である。

ー入力パラメータ

オフラインライセンス

ーLRL制御部

オフラインライセンスを格納する場合、オフラインライセンス生成済みのライセンスの情報（送信元個別公開鍵証明書のサブジェクト名、オフラインライセンスIDなど）をLRL制御部を使って取得し、過去に格納済みのオフラインライセンスか否かをチェックする。LRL管理用データベースに登録済みのオフラインライセンスで有ればエラーとする。

ーライセンス制御部

LRL管理用データベースに登録済みでなければ、ライセンス制御部を使って対応するライセンス（オンラインライセンス）が登録済みでないかどうかをチェックする。ライセンス制御部では、ライセンス管理用データベースを検索し、格納しようとしているオフラインライセンスに対応するライセンスのレコードが存在すればエラーとする。

18

【0085】図12は、オンラインライセンスの格納処理の流れを示すフローチャートである。

【0086】ステップS30において、コマンド制御部は、オフラインライセンス格納機能を起動する。ステップS31において、LA機能のシリアルライズ処理（ロードモジュールの二重起動抑止、セマフォ等）をする。

【0087】ステップS32において、オフラインライセンス暗号／復号制御部は、オフラインライセンスの復号処理を行い、ステップS33において、オフラインライセンスの正当性をチェックし、ステップS34において、LRL制御部が、LRL制御用データベースをステップS32で復号したオフラインライセンスの以下のフィールドをキーとして検索する。

ーコンテンツID

ートランザクションID

ー送信元LA個別公開鍵証明書サブジェクト名

ーオフライントランザクションID1

そして、対応するオフラインライセンスが存在する場合には、同一オフラインライセンス格納済みエラーであるとしてステップS37に進む。

【0088】ステップS34において、対応するライセンスが存在しないと判断された場合には、ステップS35において、ライセンス制御部は、ライセンス管理用データベースをステップS32で復号したオフラインライセンスの以下のフィールドをキーとして検索する。

ーコンテンツID

ートランザクションID

ステップS35において、対応するライセンスが存在すると判断された場合には、同一ライセンス既存エラーであるとしてステップS37に進む。

【0089】ステップS35において、対応するライセンスが存在しないと判断された場合には、ステップS36において、ライセンス制御部は、ステップS32で復号したオフラインライセンスからライセンス管理用データベースのレコードを作成し、格納する。そして、ステップS37で、LA機能のシリアルライズを解除して、処理を終了する。

【0090】ステップS35のライセンス管理用データベースの検索処理部で該当レコードが存在する場合は、レコード内の暗号化ライセンスを復号し、コンテンツIDとトランザクションIDの値がレコード検索のキーで指定したそれぞれの値と等しくなければ、ライセンス管理用データベースが改竄されたとみなし、エラーで終了する。

【0091】ステップS34のLRL制御用データベースの検索処理部で該当レコードが存在する場合は、レコード内の暗号化ライセンスを復号し、コンテンツIDとトランザクションIDの値がレコード検索のキーで指定したそれぞれの値と等しくなければ、LRL制御用データベースが改竄されたとみなし、エラーで終了する。

【0092】ステップS36のライセンス管理用データベースのレコード作成では、オフラインライセンスを復号して取得したライセンスを当該LAの秘密鍵によって暗号化して暗号化ライセンスを作成し、それをレコードに埋め込む。

【0093】以下に、ライセンス検索機能について説明する。

ー機能概要

・全ライセンス情報取得

全ライセンスについて以下の情報を取得する。

【0094】コンテンツID、ランザクションID、送信元個別公開鍵証明書サブジェクト名（オフラインライセンスで格納された場合のみ）、アクセス条件、オフラインライセンス生成済みか否かオフラインライセンス生成済みの場合は更に以下の情報が加えられる。

【0095】送信先個別公開鍵証明書サブジェクト名・コンテンツIDによるライセンスの検索

指定されたコンテンツIDに対応するライセンスの情報を取得する。情報の内容は上と同じ。

ー方式概要

ライセンス管理用データベース並びにLRL制御用データベースのレコードを参照して、上記情報を出力する。

1) ライセンス管理での該当レコードを読み込む  
2) LRL制御用データベースの最新フラグがオンのレコードの内、1)で参照したレコードと以下のフィールドが同じものがあるか検索する。

【0096】コンテンツID、ランザクションIDなければ、ライセンス管理用データベースのレコードの内容を出力する。あれば、オフラインライセンス生成済みとして更に追加の情報を出力する。3) LRL制御用データベースを検索し、最新フラグがオンのレコードのうち、2)で検索した以外のレコードがあれば、オフラインライセンス生成済みとして情報を出力する。

【0097】オンラインライセンスの操作との整合性  
オンラインライセンスをUDAC-MBプロトコルで移動させる場合、移動先のLAでは、以下の処理を行う。

【0098】1) LRL制御用データベースのレコードを以下のキーで検索する。

【0099】コンテンツID＝オフラインライセンスのコンテンツID

ランザクションID＝オンラインライセンスのランザクションID

最新フラグ＝オン

検索対象レコードが存在する場合、そのレコードの最新フラグの値をオフにする。

【0100】2) ライセンス制御用データベースにオンラインライセンスを格納する。その際、インターネットなおフィールドの値をゼロクリアする。

【0101】・送信元LA個別公開鍵証明書サブジェクト名

・オフラインランザクションID1

この制御と上記オフラインライセンス格納機能部並びにオフラインライセンス生成機能部の処理手順により、オフラインライセンスとオンラインライセンスとが同時に流通されたり、1つのライセンスについてオフラインライセンスのオンライン化並びにオンラインライセンスのオフライン化が行われても、ライセンスが不当に消滅したり、利用可能なライセンスの複製ができてしまうことを防いでいる。

10 LA (ソフト) のディスク領域破壊に対する対処

LAのディスク領域が破壊された場合、利用者はLAを再インストールするしかない。しかし、単純に再インストールすればLAを使用可能としたのでは利用者はオフラインライセンスの生成→LAの再インストール→オフラインライセンスの格納→オフラインライセンスの生成→・・・を繰り返すことにより1つのライセンスから複数のライセンスを生成できてしまう。

【0102】上記事態を防ぐために、LAはインストール毎に個別公開鍵証明書とそれに対応する秘密鍵のペアを変更する、といった対処方法がある。ーLAの製造元は予め1利用者について数個の鍵ペアを作っておき、各々の公開鍵証明書を認証局から発行してもらっておく。ー製造元はLAを出荷時に各利用者毎に上記鍵ペアと公開鍵証明書を製品に埋め込んで出荷する。LAは1回しかインストールできない仕様にしておく。ー利用者がLAを再インストールする場合は、インターネットなどで販売元（製造元）に申請し、新たな鍵ペアが組み込まれた新たなパッケージを受け取る。

【0103】上記以外に、LAのインストールプログラムの中で製造元のサーバと通信して新たな鍵ペアを受け取る、という方式もあるが、セキュリティ上の危険度が大きくなる。

【0104】以下に、電子文書流通へのオフラインライセンスの適用事例を示す。

【0105】UDAC-MBの従来のライセンスは、オンライン型であり、ネットワーク上でライセンスを流通させるためには、転送機能自体がUDAC-MBの転送プロトコルを実装している必要があった。そのため、ライセンスを一般の市販ソフトにより転送することができない。

【0106】オフライン型ライセンスは、ライセンスそのものは一般のソフトで転送可能である。

【0107】図13は、オフライン型ライセンスを導入した電子文書流通の概要を示す図である。

【0108】電子文書作成者が他者に電子文書を送信し、参照許諾を与える際の手順を以下に示す。

(1) 送信元（電子文書作成者）：作成した電子文書からLCM (License Compliant Module) を介して以下を生成する。このとき電子文書作成者は、アクセス制御情報を指定する。

一許諾を与えるためのライセンス

電子文書を復号するための秘密鍵である。

【0109】参照回数、印刷回数などのアクセス制御情報も付加されている。

【0110】ライセンスはLAの中に保存され、TRMを破らない限り外には出せない。

一暗号化データ

電子文書を上記ライセンスで暗号化したもの。

【0111】SCDF形式(Super Content Distribution Format)

(2) 送信元、送信先:

送信元は、電子文書送り先の利用者からLAの公開鍵証明書进行をもらう。

(3) 送信元: (2) で取得した送信先の公開鍵証明書と(1) で生成されたライセンスを指定して、LCMの機能を使ってオフラインライセンスを生成する。

【0112】オフラインライセンスは送信元のLAで生成された秘密鍵で暗号化されたライセンスと、その秘密鍵を送信先の公開鍵で暗号化したものから構成されており、そのままネットワーク上で持ち回ることが可能である。

【0113】ただし、オフラインライセンスの対攻撃強度は鍵の多重化により調整可能である。具体的にいくつの鍵で保護するかについては当業者が実装検討で決定する。

(4) 送信元、送信先: 送信元オフラインライセンスと暗号化データを送信先に送る。

【0114】送る手段はなんでもよい。(ネットワーク、可搬記録媒体)

(5) 送信先: LCMの機能を使ってオフラインライセンスをTRM領域に格納する。

(6) 送信先: 暗号化データと対応するライセンスを指定してUDAC準拠の電子文書処理アプリを実行する。

【0115】LAの秘密鍵はTRM領域内にある。また、オフラインライセンスのTRM領域への格納処理もTRM領域内で行われる。従って、送信先において送られてきた電子文書を複写することができない(TRMを破るか、もしくは、LAの秘密鍵を破らない限り)。

【0116】図14及び図15は、マルチキャスト(放送)へのオフラインライセンスの適用事例を示す図である。

【0117】なお、同図の映像音声の送信はMEPG2のフォーマットに乗っ取っているとする。

1) 契約時に各利用者は放送業者に受信チューナのLAの個別公開鍵証明書を登録する(渡す)。チューナに本実施形態のLAが内蔵されている。

2) 契約直後のチューナ電源投入時

Liは利用者iのLA個別公開鍵で生成されたオフラインライセンスである。

【0118】全契約者数分のLi(オフラインライセン

ス)をEMM(Entitlement Management Message:資格情報(放送の場合は契約情報となる))で15~30分毎に流す。なお、同図のECMは、Entitlement Check Messageの略で、スクランブル鍵やライセンスである。

【0119】本適用例では、オフラインライセンスに個別契約者情報を付加し、ライセンス管理用データベースでも個別契約者情報のフィールドを追加しているものとする。

10 【0120】LAの中のライセンス管理用データベース内のライセンスと個別契約者情報はペアでUDAC-MBプロトコルによりデコーダに送られる。

【0121】デコーダはチューナから送られてきた暗号化データをライセンスによって復号し再生する。

【0122】契約上再生可能かどうかは、デコーダ内部で受信中の番組の番組情報と個別契約情報の内容から判定する。

【0123】本方式の場合、放送局と利用者側(LA)が秘密鍵を共有するわけではないので、1つのチューナで複数の(オフラインライセンス方式を導入している)放送局の放送を受信可能である。当然ながらICカードも必要ない。

【0124】図16は、本発明の実施形態をプログラムで実現する場合に必要なとされるコンピュータのハードウェア環境図である。

【0125】CPU21は、バス20で接続された、ハードディスクなどの記憶装置27あるいは、読み取り装置28によって読み込まれる、フロッピー(登録商標)ディスク、CD-ROM、DVDなどの可搬記録媒体29に格納されたプログラムをRAM23にコピーし、実行する。また、ROM22にプログラムを格納し、コンピュータを専用のマシンとして使っても良い。なお、ROM22には、BIOSなどの基本プログラムが格納されている。

【0126】入出力装置30は、ディスプレイ、キーボード、マウス、テンプレートなどであり、ユーザの指示をCPU21に伝えると共に、処理結果をユーザに提示する。

【0127】通信インターフェース24は、ネットワーク25を介して情報提供者26と通信することにより、情報提供者26が有している記録媒体に格納された当該プログラムをダウンロードすることができる。このようにして、ダウンロードされた当該プログラムは、記憶装置27あるいは、可搬記録媒体29に格納される。あるいは、通信インターフェース24を使って、通信を行ったまま、ネットワーク環境下で当該プログラムを実行することが可能である。

【0128】なお、本実施形態のPCをコンピュータで実現する場合には、TRM領域を構成する必要があるが、これは、CPU21によって実行されるプログラム

によって構成されても良いし、あるいは、バス 20 にハードウェアで構成された T R M チップを接続して、オフラインライセンスの処理などを専門に処理させるようにしても良い。

【0129】なお、本発明の実施形態で使用する U D A C - M B / L B については、多くの特許出願がなされており、K d M 規格として知られている。以下に、幾つかの特許出願を示す。

- ・特願平 0 5 - 2 5 7 8 1 6 号
- ・特願平 0 8 - 1 0 1 8 6 7 号
- ・特願平 0 8 - 1 0 6 3 8 2 号
- ・特願平 0 8 - 1 9 0 5 2 9 号
- ・特願平 1 1 - 0 9 9 4 8 2 号
- ・特願平 0 4 - 0 5 8 0 4 8 号
- ・特願平 0 6 - 2 3 8 0 6 0 号
- ・特願平 0 6 - 2 2 5 2 2 8 号
- ・特願平 0 7 - 0 0 1 7 9 8 号
- ・特願平 1 1 - 0 9 9 4 8 2 号

（付記 1）暗号化コンテンツのライセンスをユーザ間で流通する際に用いる情報端末であって、暗号化コンテンツのライセンスを格納する第 1 の格納手段と、オフラインライセンスの生成ログを格納する第 2 の格納手段と、暗号化コンテンツのライセンスからオフラインライセンスを生成し、オフラインライセンスから暗号化コンテンツのライセンスを生成して前記第 1 の格納手段に格納し、オフラインライセンス毎に生成ログを作成または更新して前記第 2 の格納手段に格納するライセンスエージェント手段と、を備え、該オフラインライセンスを他の情報端末のライセンスエージェント手段との間でやりとりすることによって、コンテンツのライセンスを送信または受信することを特徴とする情報端末。

【0130】（付記 2）前記ライセンスエージェント手段は T R M 領域内にあることを特徴とする付記 1 に記載の情報端末。

【0131】（付記 3）前記ライセンスエージェント手段は、第 1 の格納手段内のライセンスを送付先の公開鍵とセッション鍵を使って暗号化して一般電子ファイルの形で取り出す機能を有することを特徴とする付記 1 又は 2 に記載の情報端末。

【0132】（付記 4）前記ライセンスエージェント手段は、ユーザが使用可能なライセンスの複製が生成されずに同一のオフラインライセンスを生成可能であることを特徴とする付記 1 ～ 3 のいずれか 1 つに記載の情報端末。

【0133】（付記 5）前記ライセンスエージェント手段は、オフラインライセンス受信時に、前記生成ログを用いて、移動済みのライセンスが再度格納されることを防止することを特徴とする付記 1 ～ 4 のいずれか 1 つに記載の情報端末。

【0134】（付記 6）暗号化された放送信号を用いて

複数の視聴者に対して同報されるコンテンツのライセンスを受信する際に用いる情報端末であって、コンテンツのライセンスを格納する格納手段と、受信したオフラインライセンスからコンテンツのライセンスを生成し、前記格納手段に格納するライセンスエージェント手段と、を備え、前記放送信号には全視聴契約者のオフラインライセンスが適当な間隔で挿入され、前記情報端末に対応するオフラインライセンスから、暗号化された放送信号を参照可能にするためのライセンスを生成することを特徴とする情報端末。

【0135】（付記 7）前記格納手段と前記ライセンスエージェント手段は T R M 領域内にあることを特徴とする付記 6 に記載の情報端末。

【0136】（付記 8）情報端末を用いて暗号化コンテンツのライセンスをユーザ間で流通する方法であって、暗号化コンテンツのライセンスを第 1 の格納手段に格納するステップと、前記格納された暗号化コンテンツのライセンスからオフラインライセンスを生成するステップと、前記オフラインライセンスの生成ログを作成または更新して第 2 の格納手段に格納するステップと、前記オフラインライセンスを他の情報端末に送るステップとを有するライセンスの流通方法。

【0137】（付記 9）情報端末を用いて暗号化コンテンツのライセンスをユーザ間で流通する方法であって、オフラインライセンスを他の情報端末から受け取るステップと、受け取ったオフラインライセンスから暗号化コンテンツのライセンスを生成するステップと、前記生成したライセンスを第 1 の格納手段に格納するステップと、前記オフラインライセンスの生成ログを作成または更新して第 2 の格納手段に格納するステップと、を有することを特徴とするライセンスの流通方法。

【0138】（付記 10）前記オフラインライセンスの生成及び情報端末間のオフラインライセンスのやりとりは、オフラインライセンス生成ステップを行う各情報端末中のライセンスエージェント手段を用いて行うことを特徴とする付記 8 に記載のライセンスの流通方法。

【0139】（付記 11）前記オフラインライセンスの生成及び情報端末間のオフラインライセンスのやりとりは、ライセンス生成ステップを行う各情報端末中のライセンスエージェント手段を用いて行うことを特徴とする付記 9 に記載のライセンスの流通方法。

【0140】（付記 12）前記ライセンスエージェント手段は、オフラインライセンスから暗号化コンテンツのライセンスを生成するときに、前記生成ログを用いて、移動済みのライセンスが再度保持されることを防止することを特徴とする付記 11 に記載のライセンスの流通方法。

【0141】（付記 13）暗号化された放送信号を用いて複数の視聴者に対して同報されるコンテンツのライセンスを流通する方法であって、全視聴契約者のオフライ

ンライセンスが適当な間隔で挿入された前記放送信号を受信するステップと、前記放送信号から視聴契約者の情報端末に対応するオフラインライセンスを抽出するステップと、前記抽出したオフラインライセンスから放送信号を参照可能とするためのライセンスを生成するステップと、を有することを特徴とするライセンスの流通方法。

【0142】（付記14）暗号化された放送信号を用いて複数の視聴契約者に対して同報されるコンテンツのライセンスを流通する方法であって、放送信号を暗号化するステップと、全視聴契約者にそれぞれ対応し、前記暗号化された放送信号を参照可能とするためのライセンスを生成するのに用いるオフラインライセンスを適当な間隔で挿入した前記放送信号を送信するステップと、を有することを特徴とするライセンスの流通方法。

【0143】（付記15）暗号化コンテンツのライセンスをユーザ間で流通する方法を情報端末に実現させるプログラムであって、暗号化コンテンツのライセンスを第1の格納手段に格納するステップと、前記格納された暗号化コンテンツのライセンスからオフラインライセンスを生成するステップと、前記オフラインライセンスの生成ログを作成または更新して第2の格納手段に格納するステップと、前記オフラインライセンスを他の情報端末に送るステップとを有することを特徴とするライセンスの流通方法を情報端末に実現させるプログラム。

【0144】（付記16）暗号化コンテンツのライセンスをユーザ間で流通する方法を情報端末に実現させるプログラムであって、オフラインライセンスを他の情報端末から受け取るステップと、受け取ったオフラインライセンスから暗号化コンテンツのライセンスを生成するステップと、前記生成したライセンスを第1の格納手段に格納するステップと、前記オフラインライセンスの生成ログを作成または更新して第2の格納手段に格納するステップと、を有することを特徴とするライセンスの流通方法を情報端末に実現させるプログラム。

【0145】（付記17）暗号化コンテンツのライセンスをユーザ間で流通する方法を情報端末に実現させるプログラムを格納した記録媒体であって、暗号化コンテンツのライセンスを第1の格納手段に格納するステップと、前記格納された暗号化コンテンツのライセンスからオフラインライセンスを生成するステップと、前記オフラインライセンスの生成ログを作成または更新して第2の格納手段に格納するステップと、前記オフラインライセンスを他の情報端末に送るステップとを有することを特徴とするライセンスの流通方法を情報端末に実現させるプログラムを格納した記録媒体。

【0146】（付記18）暗号化コンテンツのライセンスをユーザ間で流通する方法を情報端末に実現させるプログラムを格納した記録媒体であって、オフラインライセンスを他の情報端末から受け取るステップと、受け取

ったオフラインライセンスから暗号化コンテンツのライセンスを生成するステップと、前記生成したライセンスを第1の格納手段に格納するステップと、前記オフラインライセンスの生成ログを作成または更新して第2の格納手段に格納するステップと、を有することを特徴とするライセンスの流通方法を情報端末に実現させるプログラムを格納した記録媒体。

【0147】

【発明の効果】本発明によれば、電子データのライセンスをオフライン化したことにより、電子データの使用ライセンスを安全に受信者に渡し、不法なコピーを抑制し、かつ、電子データの頒布性を良くすることができる。

【図面の簡単な説明】

【図1】本発明の実施形態の全体構成を示す図である。

【図2】LAの機能を説明する図（その1）である。

【図3】LAの機能を説明する図（その2）である。

【図4】オフラインライセンスの構成の概要を示す図である。

【図5】新規ライセンス、暗号化データ生成を説明する図である。

【図6】ライセンス管理用データベースのレコード構成を示す図である。

【図7】オフラインライセンスの生成（オフライン化）手順を示す図である。

【図8】LRL (License Revocation List) 制御用データベースのレコード内容を示す図である。

【図9】LAの動作を説明するフローチャート（その1）である。

【図10】LAの動作を説明するフローチャート（その2）である。

【図11】オフラインライセンスの格納（オンライン化）処理を説明する図である。

【図12】オンラインライセンスの格納処理の流れを示すフローチャートである。

【図13】オフライン型ライセンスを導入した電子文書流通の概要を示す図である。

【図14】マルチキャスト（放送）へのオフラインライセンスの適用事例を示す図（その1）である。

【図15】マルチキャスト（放送）へのオフラインライセンスの適用事例を示す図（その2）である。

【図16】本発明の実施形態をプログラムで実現する場合に必要とされるコンピュータのハードウェア環境図である。

【図17】従来のライセンスを管理するための専用データ転送システムを示す図である。

【図18】従来の有料コンテンツのマルチキャストの仕組みを示す図である。

【符号の説明】

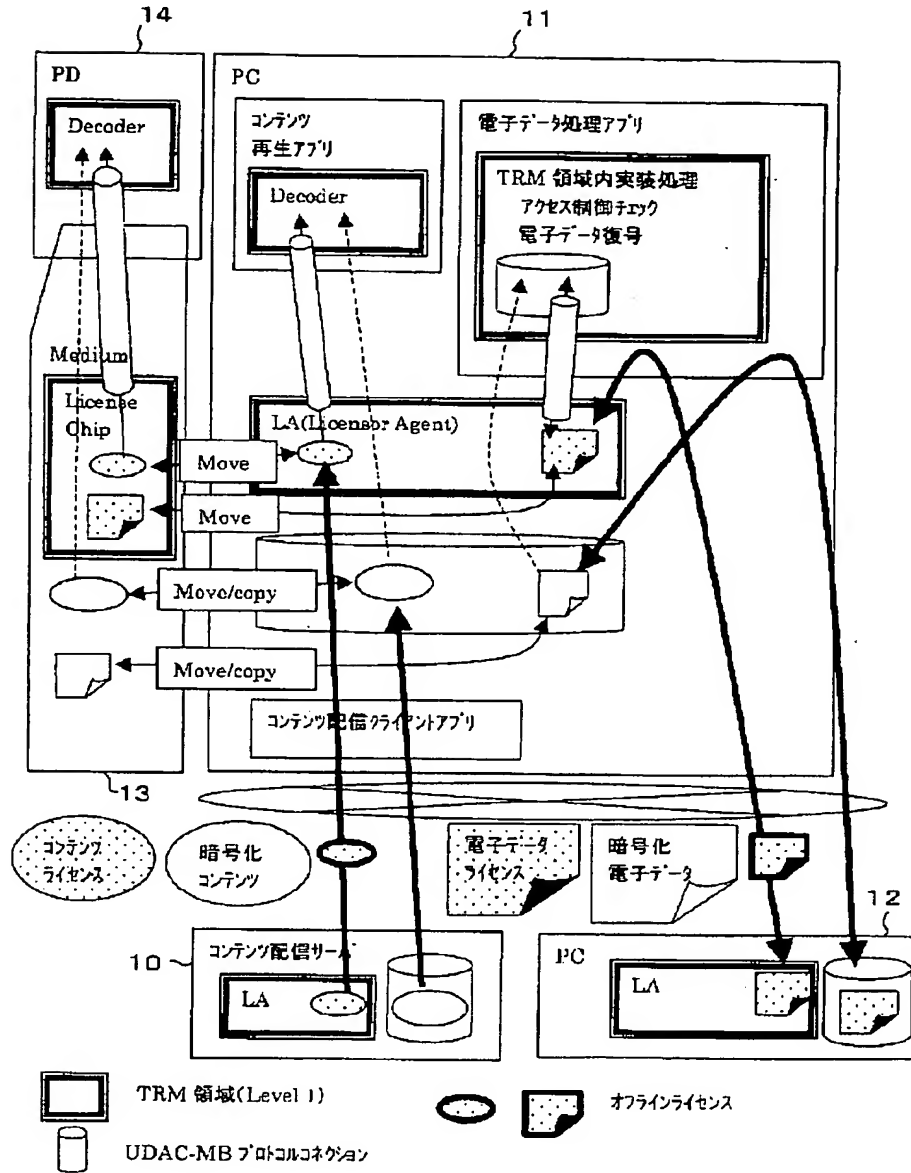
10 コンテンツ配信サーバ

11、12 PC  
13 媒体

14 PD

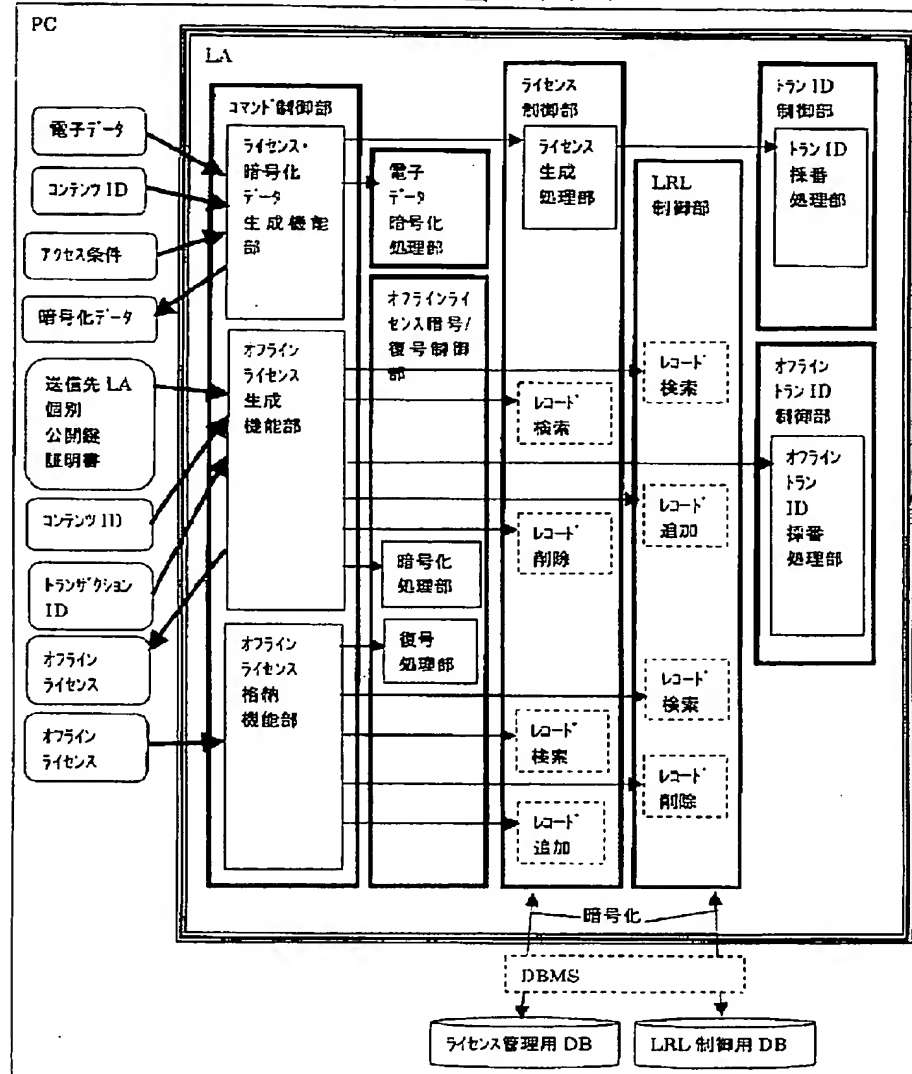
【図1】

本発明の実施形態の全体構成を示す図



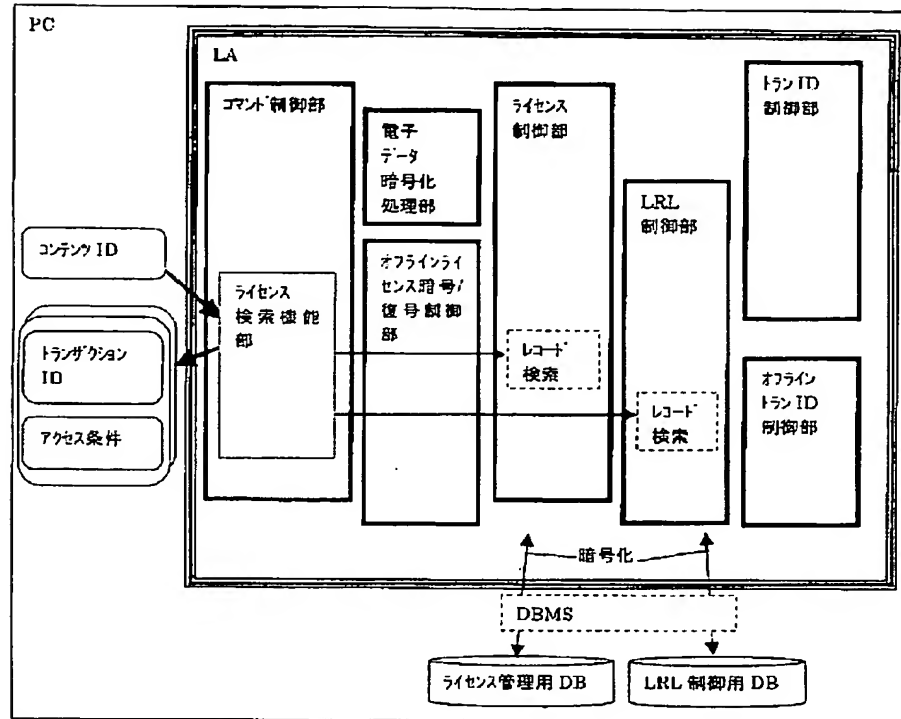
【図 2】

LAの機能を説明する図 (その1)



【図 3】

LA の機能を説明する図 (その 2)



【図 4】

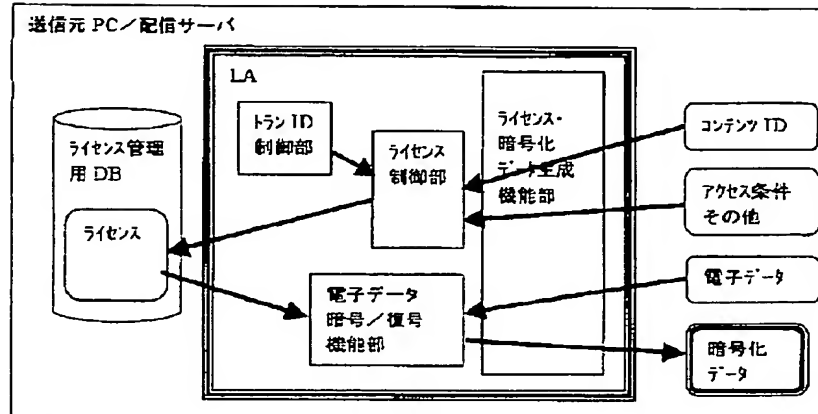
オフラインライセンスの構成の概要を示す図

Part 1	Part 2	Part 3	Part 4	Part 5
--------	--------	--------	--------	--------

- Part 1 : セッション鍵を送信先 LA の個別公開鍵で暗号化したもの
- Part 2 : 以下のデータをセッション鍵で暗号化したもの
- オフラインライセンス生成元 (送信元) LA の個別公開鍵証明書サブジェクト名
  - オフライン トランザクション ID
  - オフラインライセンス生成元 (送信元) LA で採番したもの
  - ライセンス (オンラインライセンス)
  - 配信先 TRM 内アクセス条件
  - オフラインライセンスによる移動可能回数/期間
  - その他
  - コンテンツ再生・電子データ処理システムの TRM 内アクセス条件
  - その他
- Part 3 : オフラインライセンス生成元 (送信元) LA のクラス秘密鍵による電子署名
- Part 4 : オフラインライセンス生成元 (送信元) LA の個別公開鍵証明書
- Part 5 : オフラインライセンス生成元 (送信元) LA のクラス公開鍵証明書

【図5】

新規ライセンス、暗号化データ生成を説明する図



【図6】

ライセンス管理用データベースのレコード構成を示す図

タイム スタンプ 1	コンテンツ ID	トラン ザクション ID	暗号化 ライセンス	送信元 公開鍵 証明書 サブジェクト 名	オフライン トラン ザクション ID1	タイム スタンプ 2
固定						

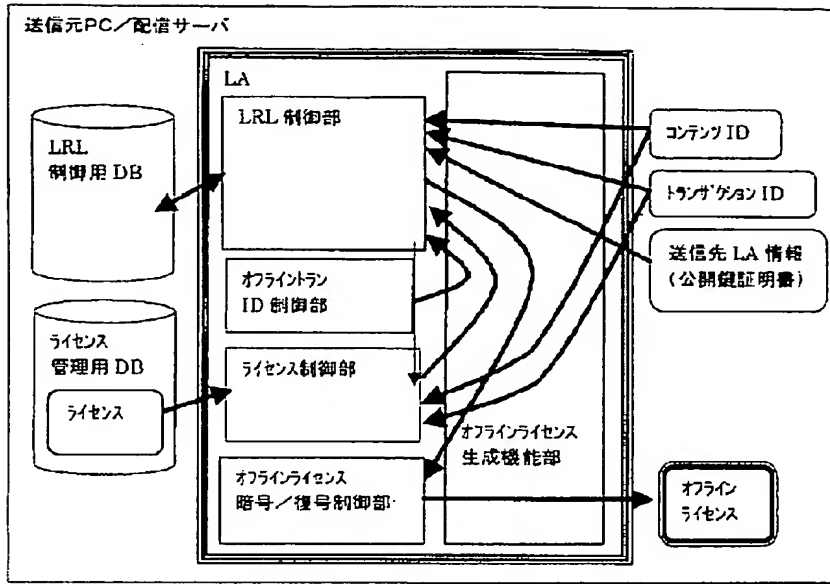
【図8】

LRL (License Revocation List) 制御用データベースの  
レコード内容を示す図

タイム スタンプ 1	コンテンツ ID	トラン ザクション ID	暗号化 ライセンス	送信元 公開鍵 証明書 サブジェクト 名	オフライン トラン ザクション ID1	送信元 公開鍵 証明書 サブジェクト 名	オフライン トラン ザクション ID2	最新 フラグ	タイム スタンプ 2
固定長									

【図 7】

オフラインライセンスの生成（オフライン化）手順を示す図

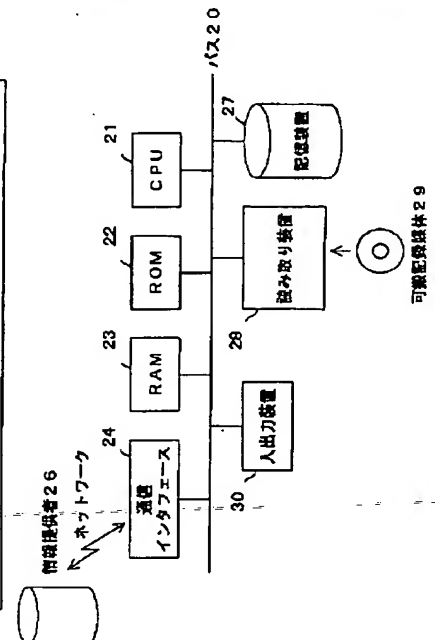
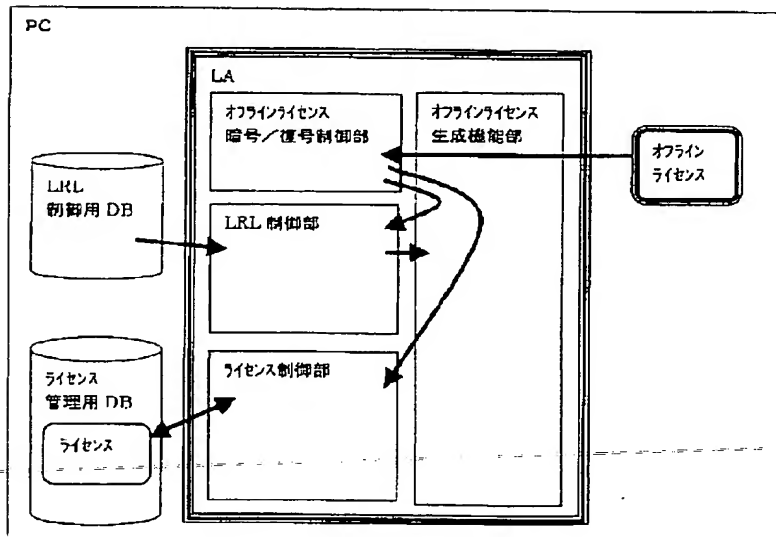


【図 11】

【図 16】

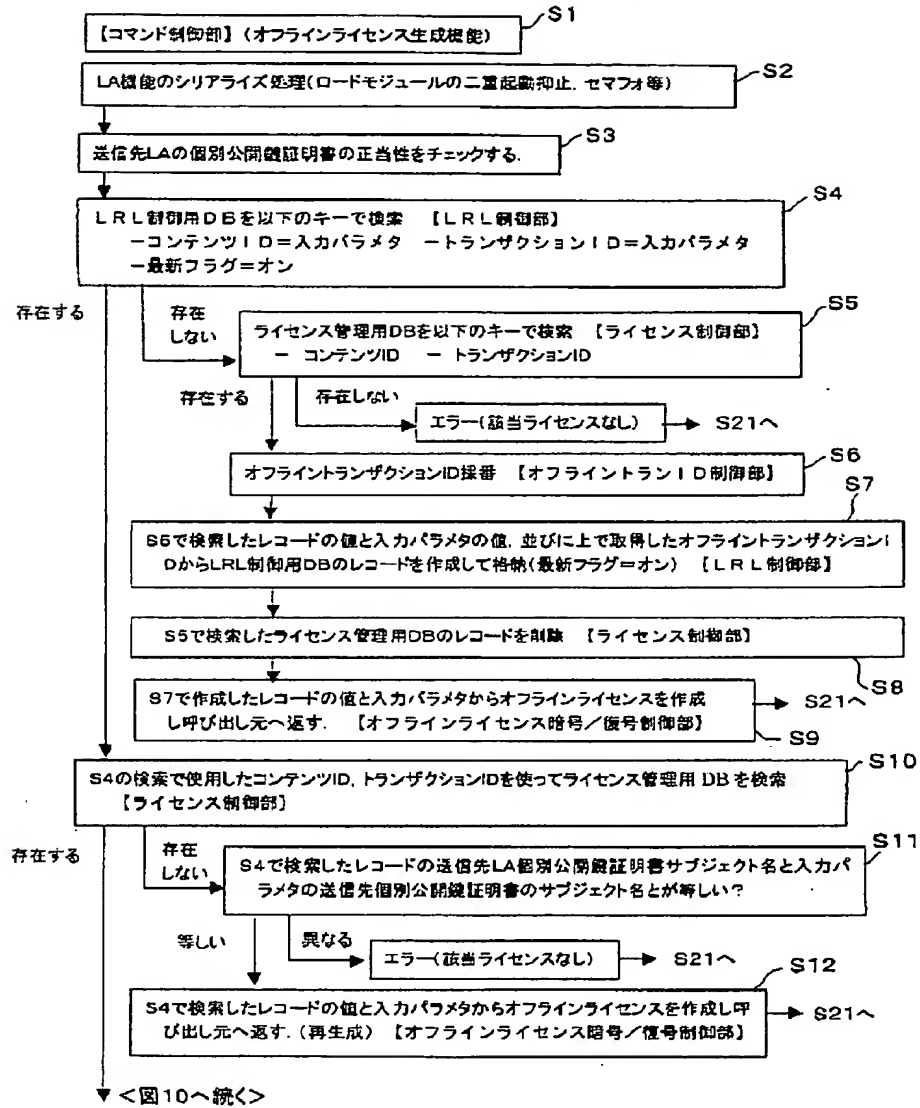
オフラインライセンスの格納（オンライン化）処理を説明する図

本発明の実施形態をプログラムで実現する場合に必要なとされるハードウェア環境図



【図 9】

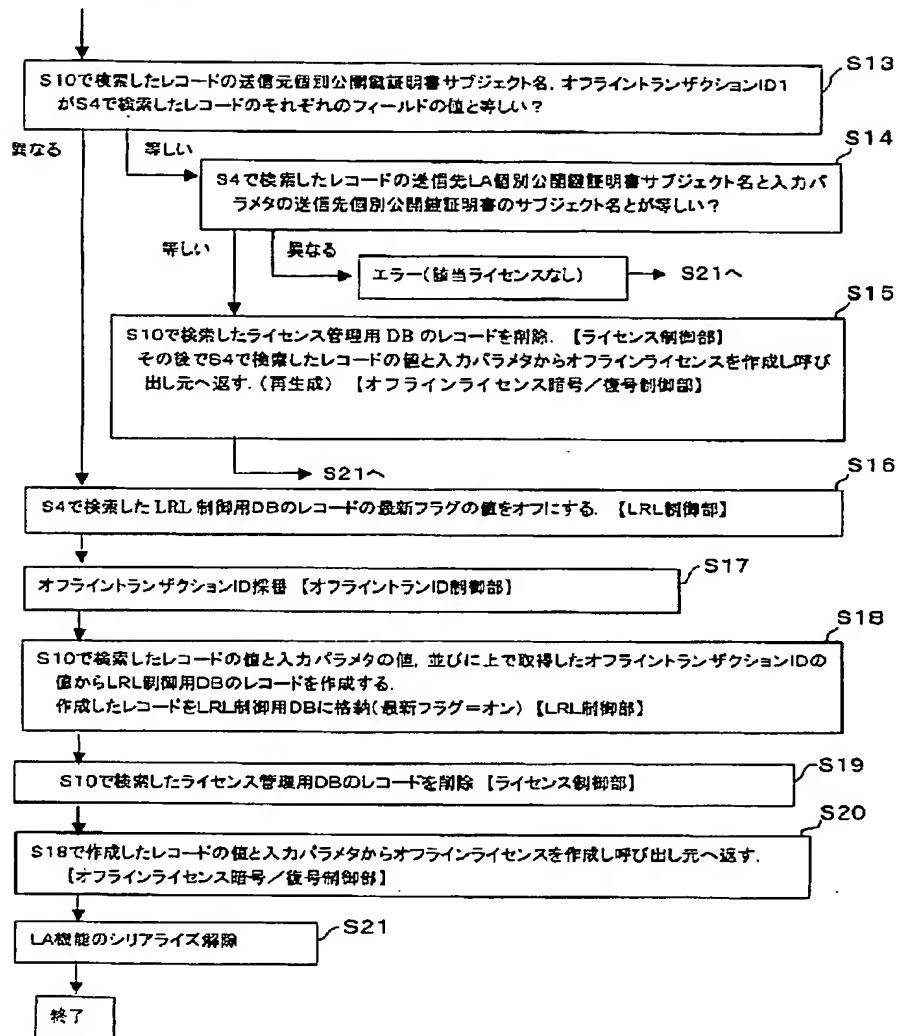
## LAの動作を説明するフローチャート（その1）



【図 10】

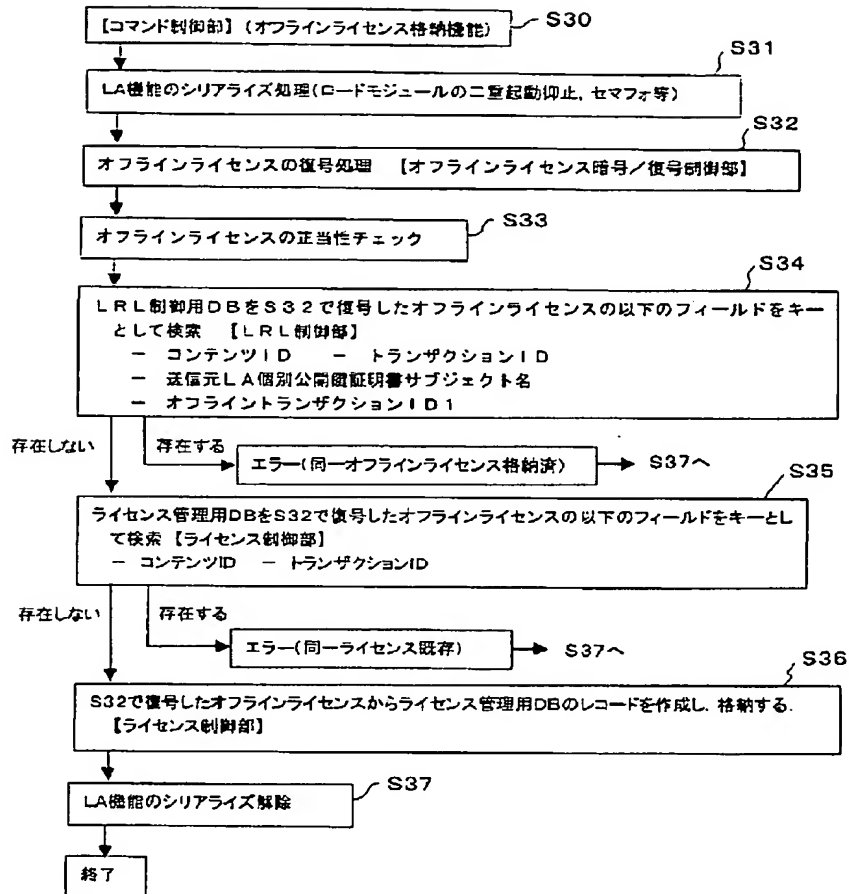
## LAの動作を説明するフローチャート（その2）

&lt;図9からの続き&gt;



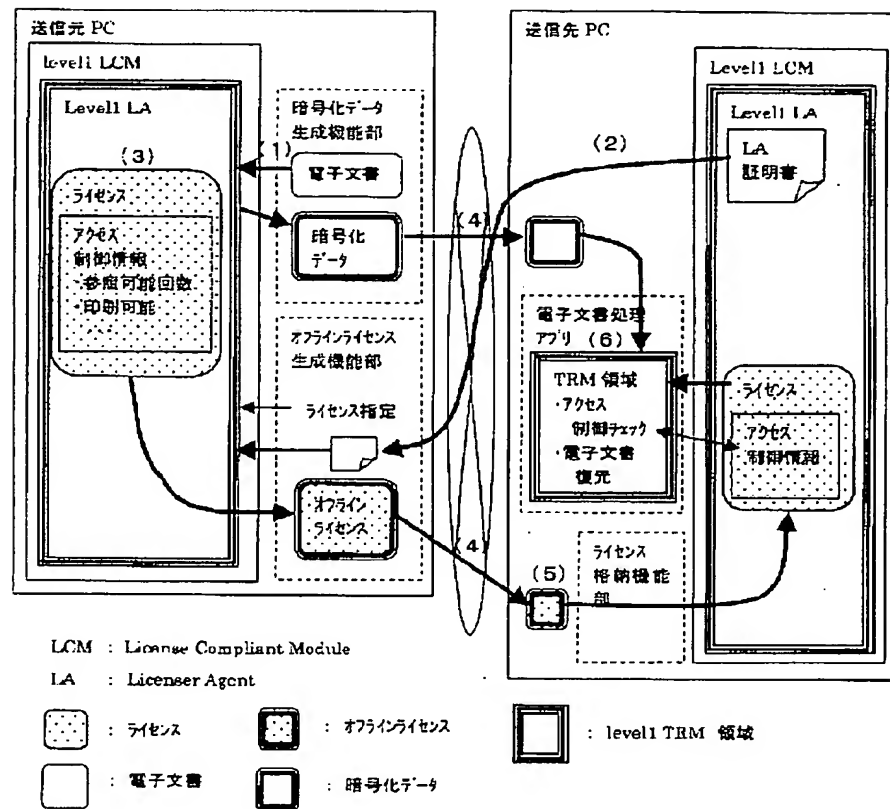
【図 12】

オンラインライセンスの格納処理の流れを示すフローチャート



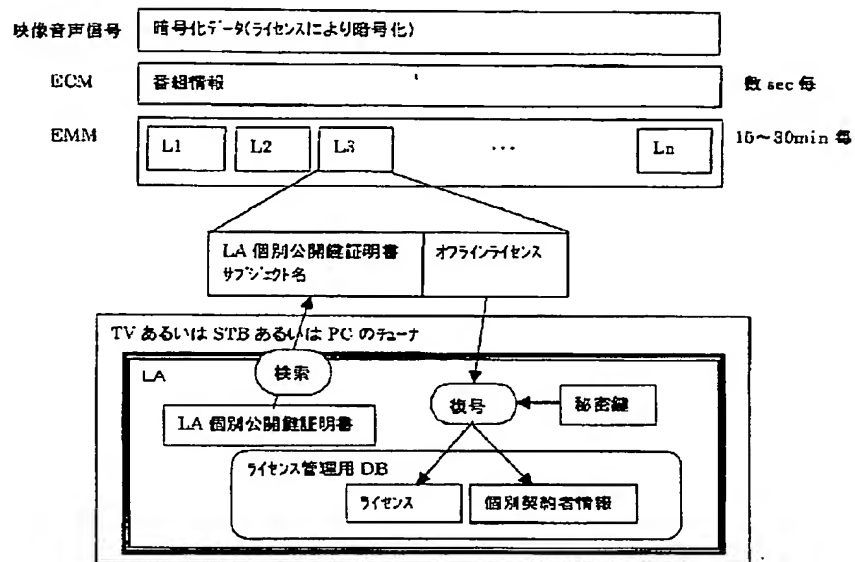
【図 13】

オフライン型ライセンスを導入した電子文書流通の概要を示す図



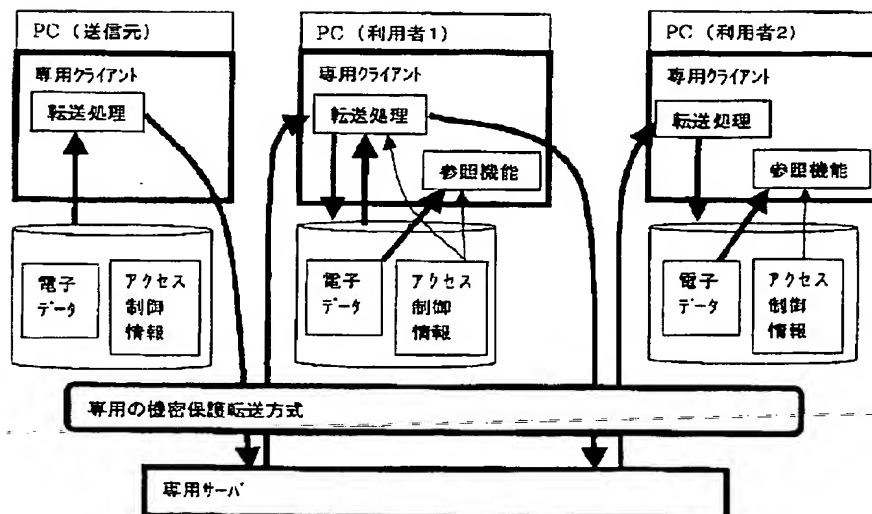
【図 14】

マルチキャスト(放送)へのオフラインライセンスの適用事例を示す図  
(その1)



【図 17】

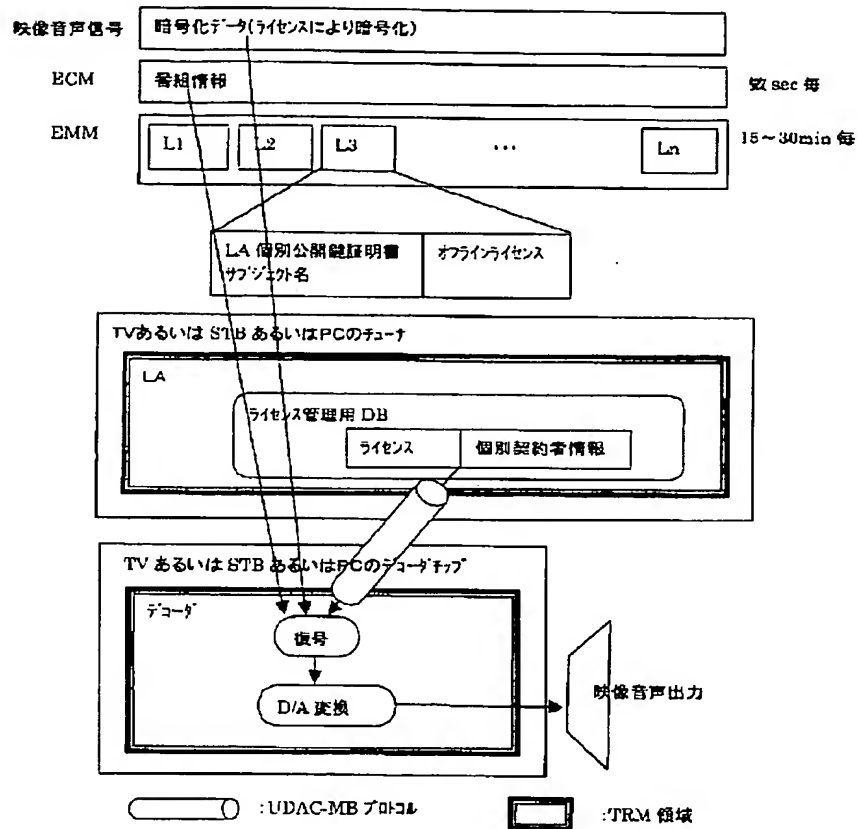
従来のライセンスを管理するための専用データ転送システムを示す図



【図 15】

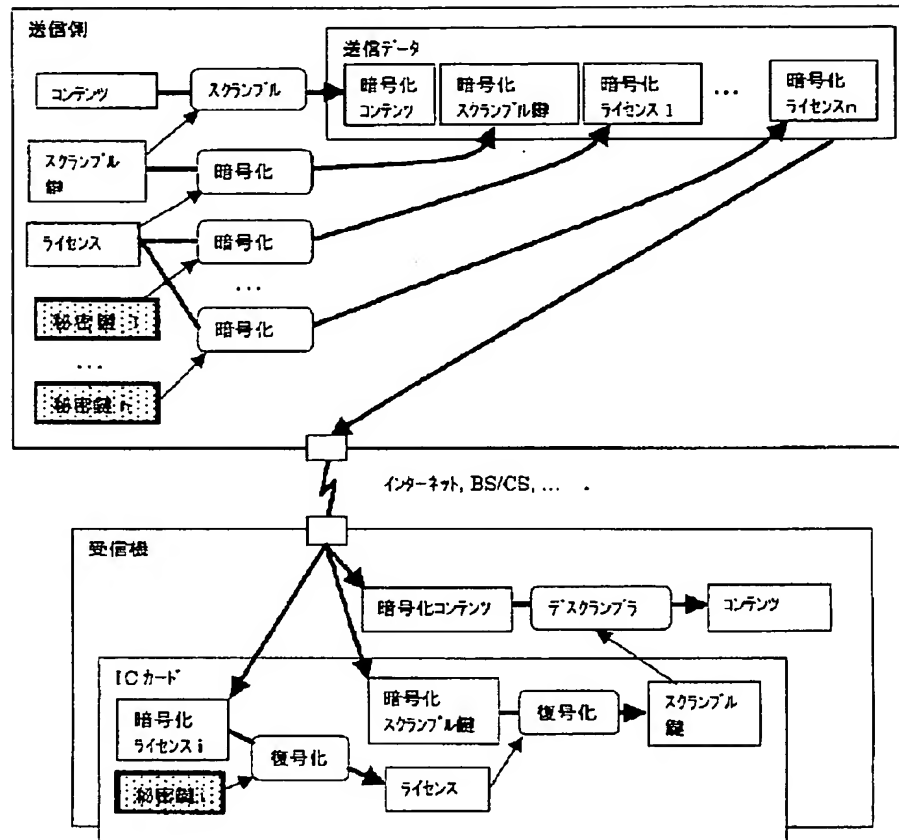
マルチキャスト(放送)へのオフラインライセンスの適用事例を示す図

(その 2)



【図18】

従来の有料コンテンツのマルチキャストの仕組みを示す図



フロントページの続き

(51) Int. Cl.<sup>7</sup>

G 0 6 F 17/60  
H 0 4 H 1/00  
H 0 4 L 9/08  
9/10

識別記号

5 1 2

F 1

H 0 4 H 1/00  
H 0 4 L 9/00  
G 0 6 F 9/06  
H 0 4 L 9/00

テーマコード(参考)

F  
6 0 1 A  
6 6 0 A  
6 2 1 A

(72) 発明者 長谷部 高行

神奈川県川崎市中原区上小田中4丁目1番  
1号 富士通株式会社内

(72) 発明者 千葉 哲央

神奈川県川崎市中原区上小田中4丁目1番  
1号 富士通株式会社内

Fターム(参考) 5B076 FA01 FC01

5B085 AE23 AE29 BC01 CA06

5J104 AA01 AA16 EA04 EA17 NA02

NA42 PA07